UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/040,156	12/19/2001	Travis M. McGregor	23758.00120	1147

7590 07/07/2004

Christopher M. McGregor
Q Technologies
Spear Tower-One Market
Suite 3600
San Francisco, CA 94105

EXAMINER	
AU, SCOTT D	

ART UNIT	PAPER NUMBER
2635	8

DATE MAILED: 07/07/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/040,156	Applicant(s) MCGREGOR ET AL.	
	Examiner Scott Au	Art Unit 2635	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *36* is/are allowed.

6)☒ Claim(s) *1-11,13,17-22 and 24-35* is/are rejected.

7)☒ Claim(s) *12,14-16 and 23* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 April 2002* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 5.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

The application of McGregor for a "Bio-metric smart card, bio-metric smart card reader and method of use" filed December 19, 2001 has been examined.

Claims 1-36 are pending.

Drawings

The drawings are objected to because referring to system 100, slot 122 and a card reader 230 as described in the specification, the numbers are not shown on the drawing. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Objections

Claims 15-17 are objected to because of the following informalities: The limitation "device" contradicts the limitation "system" of claim 9 and 14. Examiner suggests changing the limitation "device" as to "system". Appropriate correction is required.

Specification

The disclosure is objected to because of the following informalities: On page 12, paragraph 3, presently read as "microprocessor 510 and electrical connection 516"

which the examiner suggests it should be rewritten as "microprocessor 520 and electrical connection 526" according to the Figure 5. Appropriate correction is required.

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

The present abstract uses the phrase " the present invention" which should be avoided. It does not comply with the guidelines.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-8 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "apparatus" contradict the limitation "device". There is insufficient antecedent basis for this limitation in the claim. Examiner suggests changing the limitation "apparatus" to "device".

Regarding claims 2-8 are rejected because the claims are dependent upon claim 1.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1,3-6,9,12-13,18 and 20-22 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1,3-6,8,11-13 and 15-17 of copending Application No. 09/843,572. Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant claims are generally broader than the claims in your co-pending application. See In re Van Ornum and Stang, 214, USPQ 761, 766, and 767 (CCPA) (the court sustained an obvious double patenting rejection of generic claims in a continuation application over narrower species claims in an issued patent); In re Vogel,

164 USPQ 619, 622, and 623 (CCPA 1970) (generic application claim specifying "meat" is obvious double patenting of narrow patent claim specifying "port").

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Referring to claim 1 of (Application No. 10/040,156), the copending (Application No. 09/843,572) claims a device for preventing the unauthorized use of proprietary data, the device comprising: a user authentication device configured to provide the user an authentication data input for proving the user is authorized to use the account number; a transaction counting mechanism configured to track authorized device access events; a processor device in electrical communication with the user authenticator and counter, the processor being programmed to generate a security key in response to authentication data received via the user authenticator, the security key being derived at least in part from the contents of the counter; and a display unit configured to display the security key on the apparatus.

However, the copending (Application No. 09/843,572) claims narrower that the user authenticator with a biometric authentication input, the account number is a non-varying number and the security key being derived at least in part from the content of the counter and at least in part from the user's biometric authentication data (i.e. see claim 1 of copending Application No. 09/843,572).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to include the user authenticator with a biometric

authentication input, the account number is a non-varying number and the security key being derived at least in part from the content of the counter and at least in part from the user's biometric authentication data of copending (Application No. 09/843,572) with the motivation for doing so would allow the security of a transaction.

Referring to claim 9 of (Application No. 10/040,156), the copending (Application No. 09/843,572) claims a system for securely processing transactions, the system comprising: a security key device, comprising, a user authenticator configured to provide a user an authentication data input for proving the user is authorized to use an account associated with the security device, a first counter in communication with the user authenticator, a key generator in communication with the user authenticator and first counter, the key generator being programmed to generate a security key in response to authentication data received via the user authenticator, the security key being derived at least in part from contents of the first counter, and an electronic display in electrical communication with the key generator, for displaying the security key in a manner visible upon the structure; and an authorization device, comprising, a second counter, and a key confirmation processor programmed to confirm an authenticity of the security key in a manner at least partially dependent upon the contents of the second counter.

However, the copending (Application No. 09/843,572) claims narrower that the user authenticator with a biometric authentication input, the first counter having representative of authorized device access events, the security key being derived at

least in part from the contents of the first counter and at least in part from the user's biometric authentication data, and the second counter having contents representative of successful device access events (i.e. see claim 8 of the copending Application No. 09/843,572).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to include the user authenticator with a biometric authentication input, the first counter having representative of authorized device access events, the security key being derived at least in part from the contents of the first counter and at least in part from the user's biometric authentication data, and the second counter having contents representative of successful device access events of copending (Application No. 09/843,572) with the motivation for doing so would allow the security of a transaction.

Claims 2-8, 10-13,17-22 and 24 of (Application No. 10/040,156) are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over copending (Application No. 09/843,572) as applied to claims 1 and 9, and further in view of Walker et al. (US# 6,163,771).

Referring to claims 2 and 7 of (Application No. 10/040,156), the copending (Application No. 09/843,572) claims the device of claim 1. However, (Application No. 09/843,572) did not explicitly claim wherein the security key is derived from the contents of the counter and a user's PIN.

In the field of endeavor of transaction device, Walker et al. disclose wherein the security key is derived from the contents of the counter and a user's PIN (col. 5 lines 53-60 and col. 10 line 65 to col. 11 line 7) in order to provide a valid transaction. Examiner interprets the counter is a clock device that is used in conjunction with the credit card to provide a valid transaction.

Therefore, it would have been obvious to a person of skilled in the art at the time of the invention was made to use the method of derived a security key for transaction event of Walker et al. in the transaction device of the copending (Application No. 09/843,572) with the motivation for doing so would allow the high security of deriving a valid transaction.

Referring to claim 8 of (Application No. 10/040,156), the copending (Application No. 09/843,572) in view of Walker et al. (US# 6,163,771) disclose the device of claim 1. Walker et al. disclose further comprising a clocking mechanism having an output coupled to the processor device, wherein said processing device also uses the clocking mechanism output to derive the security key (col. 10 line 65 to col. 11 line 7).

Referring to claim 3 of (Application No. 10/040,156), corresponding to (Application No. 09/843,572) claim 3.

Referring to claim 4 of (Application No. 10/040,156), corresponding to (Application No. 09/843,572) claim 4.

Referring to claim 5 of (Application No. 10/040,156), corresponding to (Application No. 09/843,572) claim 5.

Referring to claim 6 of (Application No. 10/040,156), corresponding to (Application No. 09/843,572) claim 6.

Referring to claims 10 and 11 of (Application No. 10/040,156), (Application No. 09/843,572) in view Walker et al. (US# 6,163,771) disclose a system of claim 9, claims 10-11 are equivalent to that of claims 2 and 7 addressed above, incorporated herein. Therefore, claim 10-11 are rejected for same reasons given with respected to claims 2 and 7.

Referring to claim 12 of (Application No. 10/040,156), corresponding to (Application No. 09/843,572) claim 11.

Referring to claim 13 of (Application No. 10/040,156), corresponding to (Application No. 09/843,572) claim 12.

Referring to claim 17 of (Application No. 10/040,156), the copending (Application No. 09/843,572) in view Walker et al. disclose the device of claim 9, Walker et al. disclose further wherein the authorization device is configured to retrieve the security key from a PIN field of a received transaction communication (col. 7 lines 4-19).

Referring to claim 18 of (Application No. 10/040,156), the copending (Application No. 09/843,572) claims a method of securely authorizing a transaction utilizing an account, the method comprising: confirming an authorized use of an account by a user; maintaining a first count indicative of a number of instances of such authorized uses; generating a security key in a manner at least partially dependent upon the count; transmitting the security key to an authorizing authority; processing the security key at the authorizing authority; maintaining a second count indicative of a number of transmissions received by the authorizing authority for the account; confirming that the security key was generated by an authorized user at least in part through use of the second count; and authorizing the transaction if the security key was generated by an authorized user. However, (Application No. 09/843,572) claims confirming an authorized use of an account card via a biometric sensor instead of a PIN (i.e. see claim 13 of Application No. 09/843,572).

In the same field of endeavor, Walker et al. disclose the cardholder inputs his PIN or biometric data to access the device (col. 6 lines 18-22).

Therefore, it would have been obvious to a person of skilled in the art at the time of the invention was made to include PIN input of Walker et al. in the transaction device of (Application No. 09/843,572) with the motivation for doing so would allow the PIN input means as an alternative of using biometric data input.

Referring to claim 19 of (Application No. 10/040,156), the copending (Application No. 09/843,572) in view of Walker et al. disclose the method of claim 18, Walker et al.

further disclose the method of claim 18, wherein the PIN is input by a keypad (col. 5 lines 53-60).

Referring to claim 20 of (Application No. 10/040,156), corresponding to (Application No. 09/843,572) claim 15.

Referring to claim 21 of (Application No. 10/040,156), corresponding to (Application No. 09/843,572) claim 16.

Referring to claim 22 of (Application No. 10/040,156), corresponding to (Application No. 09/843,572) claim 17.

Referring to claim 24 of (Application No. 10/040,156), the copending (Application No. 09/843,572) in view Walker et al. (US# 6,163,771) disclose a method of claim 18, claim 24 is equivalent to that of claim 17 addressed above, incorporated herein. Therefore, claim 24 is rejected for same reasons given with respected to claim 17.

Claim Rejections - 35 USC § 102

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

Claims 1-11, 13 and 17-22 are rejected under 35 U.S.C. 102(e) as being anticipated by Walker et al. (US# 6,163,771)

Referring to claim 1, Walker et al. disclose a device (100) (i.e. a smart card) for preventing the unauthorized use of proprietary data, the device (100) (i.e. a smart card) comprising: a user authentication device (103) (i.e. a keypad) configured to provide the user an authentication data input for proving the user is authorized to use the account number (col. 5 lines 49-61, col. 6 lines 1-3 and col. 8 lines 32-36; see Figures 1 and 2); a transaction counting mechanism (413) (i.e. database corresponds to initialization variable) configured to track authorized device access events (col. 7 lines 36-51 and col. 8 lines 19-29; see Figures 7-8); a processor device (101) (i.e. a central processor) in electrical communication with the user authenticator (i.e. user's private key K) and counter (413) (i.e. database corresponds to initialization variable), the processor (101) (i.e. a central processor) being programmed to generate a security key in response to authentication data received via the user authenticator, the security key being derived at least in part from the contents of the counter(413) (i.e. database corresponds to initialization variable); and a display unit (102) (i.e. display screen) configured to display the security key on the apparatus (col. 7 lines 27-51 and col. 8 lines 10-29; see Figures 1-2 and 7).

Referring to claim 2, Walker disclose the device of claim 1, wherein the security key is derived from the contents of the counter and a user's PIN (col. 6 lines 14-38, col. 7 lines 27-51, col. 8 lines 9-29 and col. 11 lines 46-62; see Figures 1 and 10).

Referring to claim 3, Walker et al. disclose the device of claim 2, further wherein the security key is encrypted before being displayed (col. 8 lines 9-36; see Figure 8).

Referring to claim 4, Walker et al. disclose the device of claim 2, further comprising a wireless transmitter to transmit the security key to a network device (col. 1 lines 43-46). (It is inherent that the transmitter is included in the device (100).

Referring to claim 5, Walker et al. disclose the device of claim 4, further comprising a smart card reader, wherein the device can be used with existing smart cards to provide a security key for transactions (col. 1 lines 35-49, col. 6 lines 15-29 and col. 7 lines 4-19). It is inherent that the merchant has a smart card reader for the smart card device (100) to process a valid transaction.

Referring to claim 6, Walker et al. disclose the device of claim 4, wherein the device is connected to a computer (i.e. authorization terminal) to authorize transactions on a network (col. 6 lines 39-53; see Figure 3A). It is inherent and known in the art that transaction device is connected to a computer for communication with the credit card issuer for processing a valid transaction.

Referring to claim 7, Walker et al. disclose the device of claim 2, wherein the user authenticator is a PIN entry system (col. 6 lines 18-29).

Referring to claim 8, Walker et al. disclose the device of claim 1, further comprising a clocking mechanism having an output coupled to the processor device, wherein said processing device also uses the clocking mechanism output to derive the security key (col. 10 line 64 to col. 11 line 7).

Referring to claim 9, Walker et al. disclose a system for securely processing transactions, the system comprising: a security key device (100) (i.e. a device or smart card), comprising, a user authenticator (103) (i.e. a keypad) configured to provide a user an authentication data input (i.e. PIN) for proving the user is authorized to use an account associated with the security device (100), a first counter (413) (i.e. database corresponds to initialization variable) in communication with the user authenticator(103), a key generator (101) (i.e. device central processor) in communication with the user authenticator (103) and first counter (413) (i.e. database corresponds to initialization variable), the key generator (101) (i.e. device central processor) being programmed to generate a security key in response to authentication data received via the user authenticator (103) (i.e. a keypad), the security key being derived at least in part from contents of the first counter(413) (i.e. database corresponds to initialization variable), and an electronic display in electrical (102) (i.e. display screen) communication with the key generator(103) (i.e. a keypad), for displaying the security key in a manner visible upon the structure (col. 5 lines 49-61, col. 7 lines 37-51 and col. 8 lines 9-36); and an authorization device (400) (i.e. issuer's central , comprising, a second counter (i.e. clock), and a key confirmation processor

(401) (i.e. CPU) programmed to confirm an authenticity of the security key in a manner at least partially dependent upon the contents of the second counter (i.e. clock) (col. 7 lines 4-19 and col. 10 line 64 to col. 11 line 7; see Figures 4 and 12).

Referring to claim 10, Walker et al. disclose a system of claim 9, wherein the security key is derived at least partially from the contents of the first counter (col. 6 lines 15-29, col. 7 lines 36-51and col. 8 lines 9-36).

Referring to claim 11, Walker et al. disclose a system of claim 9, wherein the security key is derived at least partially from the contents of the first counter and a user PIN (col. 6 lines 15-29, col. 7 lines 36-51and col. 8 lines 9-36).

Referring to claim 13, Walker et al. disclose a system of claim 10, further wherein the security key is encrypted before being displayed and the key confirmation processor decrypts the key in order to authenticate a transaction (col. 8 lines 9-65; see Figures 8 and 9B).

Referring to claim 17, Walker et al. disclose a system of claim 9, wherein the authorization device is configured to retrieve the security key from a PIN field of a received transacton communication (col. 6 lines 18-29 and col. 11 lines 46-51).

Referring to claim 18, Walker et al. disclose a method of securely authorizing a transaction utilizing an account, the method comprising: confirming an authorized use of an account card via a PIN provided by a user (col. 11 lines 46-62); maintaining a first count indicative of a number of instances of such authorized uses (col. 7 lines 46-51); generating a security key in a manner at least partially dependent upon the count (col. 8 lines 9-36); transmitting the security key to an authorizing authority (col. 8 lines 31-40); processing the security key at the authorizing authority (col. 8 lines 41-65); maintaining a second count indicative of a number of transmissions received by the authorizing authority for the account (col. 10 line 63 to col. 11 line 7); confirming that the security key was generated by an authorized user at least in part through use of the second count (col. 10 line 63 to col. 11 line 20); and authorizing the transaction if the security key was generated by an authorized user (col. 12 lines 39-42).

Referring to claim 19, Walker et al. disclose a method of claim 18, wherein the PIN is input by a keypad (col. 11 lines 46-49; see Figures 1-2).

Referring to claim 20, Walker et al. disclose a method of claim 18, wherein the security key is generated using an encryption algorithm to process a card key and the first count (col. 7 lines 36-51 and col. 8 lines 9-40).

Referring to claim 21, Walker et al. disclose a method of claim 20, wherein the transaction is authorized if the first count is within a predefined number of the second count (col. 11 lines 1-7).

Referring to claim 22, Walker et al. disclose a method of claim 21, wherein the card key is generated from a master key provided by the account provider and from a user's bio-metric data (col. 6 lines 18-29).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 25 and 29-31 are rejected under 35 U.S.C. 102(b) as being anticipated by Pavlov et al. (US# 4,614,861).

Referring to claim 25, Pavlov et al. disclose a smart card, comprising,

an activation device (12) (i.e. keypad) configured to produce a signal in response to a user action (col. 11 lines 30-38; see Figure 3);

a display mechanism (14) (i.e. display) (col. 12 lines 12-25);

a processing device (34) (i.e. microprocessor) coupled to the display device (14) (i.e. display) and configured to receive said signal (col. 9 lines 47-57; see Figure 3); and programming executed by the processing device (col. 10 lines 35-38), said programming configured to produce an encrypted key and display the encrypted key on the display mechanism (col. 7 lines 4-15 and col. 16 lines 47-65).

Referring to claim 29, Pavlov et al. disclose the smart card according to claim 25, wherein said activation device is a button (col. 9 line 48 to col. 10 line 7;see Figures 1, 3 and 5).

Referring to claim 30, Pavlov et al. disclose the smart card according to claim 25, wherein said activation device is a ten key type entry system and said user action is entry of a PIN (col. 12 lines 12-20).

Referring to claim 31, Pavlov et al. disclose the smart card according to claim 25, wherein: said programming is further configured to verify said user action prior to displaying the encrypted key; and if said programming is unable to verify said user action, then, displaying one of an error message and a non-authentic value (col. 12 lines 1-11).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pavlov et al. (US# 4,614,861) as applied to claim 25 above, and further in view of Draggar (US# 5,748,737).

Referring to claim 26, Pavlov et al. disclose the smart card according to claim 25. However Pavlov et al. did not explicitly disclose wherein: said smart card comprises a credit card sized enclosure; said display mechanism is disposed on a face of the credit card sized enclosure; and said programming is stored on a computer readable media disposed on or within the credit card sized enclosure.

In the same field of endeavor of smarts card data carrier means, Draggar discloses wherein: said smart card comprises a credit card sized enclosure (100); said display mechanism (110) is disposed on a face of the credit card sized enclosure (100) (col. 10 lines 30-44; see Figure 1); and said programming is stored on a computer readable media disposed on or within the credit card sized enclosure (col. 2 lines 10-15) in order to allow the card exchange data with the card data carrier means.

One of ordinary skill in the art understands that card data carrier means of Dragger is desirable in the transaction card of Pavlov et al. because Pavlov et al. suggest card 10 can be inserted through card reader slot 104 which reads the magnetic stripe from the back of the card. A person validating the card can compare the account number appearing on screen 106, which is read from the magnetic stripe of card 10, with the account number appearing on the display 14 of the card and the embossed number of the card. If all three account numbers correspond, the account number read from the card can be compared electronically with the stored account numbers to validate use of card 10. Keypad 108 can additionally be used for entering the transaction identification code (TIC) and/or the personal identification number (PIN) to verity proper use of card 10 by verifying the validity of the transaction identification code (col. 16 lines 12-26) and Dragger teaches an electronic wallet 100 includes data processing means, data storage means, and media interface means. Preferably, electronic wallet 100 is formed from plastic, metal or other suitable material, and may for example have dimensions approximately 63 mm by 92.5 mm by 4 mm. Dragger further discloses a keypad 120 and display 110 provide user interface means. Similarly a card slot 130 provided in the wallet 100 allows any card 150 to be inserted into the electronic wallet 100 so that data exchange via a card medium/wallet medium interface can occur (col. 10 lines 30-42). Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to include cad data carrier means of Dragger in the transaction card of Pavlov et al. with

the motivation for doing so would allow the person the convenience of making payments and obtaining funds.

Referring to claim 27, Pavlov et al. in view of Dragger disclose the smart card according to claim 26, Dragger disclose further wherein said credit card sized enclosure in a solid flexible material (col. 10 lines 30-44).

Referring to claim 28, Pavlov et al. in view of Dragger disclose the smart card according to claim 26, Dragger disclose further wherein said activation device is a numeric entry system disposed on a face of the credit card sized enclosure (col. 10 lines 38-44; see Figure 1).

Claims 32-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pavlov et al. (US# 4,614,861) as applied to claim 25 above, and further in view of Walker et al. (US# 6,163,771).

Referring to claim 32, Pavlov et al. disclose the smart card according to claim 25. However, Pavlov et al. did not explicitly disclose further comprising: a bio-metric sensing device coupled to said processing device; wherein: said programming is further configured to, retrieve a bio-metric input from said bio-metric sensing device and compare the bio-metric input to a stored bio-metric value prior to one of calculating and displaying the encrypted key, and verify said user action prior to displaying the

encrypted key prior to one of calculating and displaying the encrypted key; and if said comparison of the bio-metric input does not match the bio-metric value, or, if the user action is not verified, then, displaying one of an error message and a non-authentic value instead of the encrypted key.

In the same field of endeavor of transaction card, Walker et al. disclose a bio-metric sensing device (105) (i.e. biometric interface) coupled to said processing device (101) (central processor); wherein: said programming is further configured to, retrieve a bio-metric input from said bio-metric sensing device (105) (i.e. biometric interface) and compare the bio-metric input to a stored bio-metric value prior to one of calculating and displaying the encrypted key, and verify said user action prior to displaying the encrypted key prior to one of calculating and displaying the encrypted key (col. 4 lines 5-21 and col. 6 lines 18-29); and if said comparison of the bio-metric input does not match the bio-metric value, or, if the user action is not verified, then, displaying one of an error message and a non-authentic value instead of the encrypted key.

One of ordinary skill in the art understands that biometric sensing device of Walker et al. is desirable in the self-contained card of Pavlov et al. because Pavlov et al. suggest the card holder to enter his personal identification number (PIN). Prompting is provided by displaying a message (ENTER PIN) on display 14. The card user is then expected to enter the personal identification number (PIN) using keypad 12. The entered personal identification number (PIN) is then compared with the personal identification number (PIN) stored in memory during programming of the

device. If there is an incorrect match of the two personal identification number (PIN)s, the number of consecutive wrong guesses is incremented by one. A check is performed to determine if the maximum allowable number of guesses has been exceeded. If it has been, the card is invalidated by setting the invalid flag and a message is displayed on the device's display indicating that the card is invalid. The card is then powered down and disabled from further use (col. 11 line 62 to col. 12 line 11). And Walk et al. teach the device may be activated through the input of a unique cardholder identifier such as a personal identification number (PIN) through the keypad 103. Alternatively, the device may include a biometric interface 105, and be activated by the input of a suitable biometric record such as the cardholder's fingerprint (col. 5 lines 53-61). Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to include a biometric interface coupled to said central processor; wherein: said programming is further configured to, retrieve a bio-metric input from said biometric interface and compare the bio-metric input to a stored bio-metric value prior to one of calculating and displaying the encrypted key, and verify said user action prior to displaying the encrypted key prior to one of calculating and displaying the encrypted key in the self-contained card of Pavlov et al. with the motivation for doing so would allow biometric identification as an alternative of keypad input.

Referring to claim 33, Pavlov et al. in view of Walker et al. disclose the smart card according to claim 32, Walker et al. disclose further wherein said bio-metric sensing device is a fingerprint scanner (col. 5 lines 55-61).

Referring to claim 34, Pavlov et al. in view of Walker et al. disclose the smart card according to claim 25, Walker et al. disclose further comprising: a clocking mechanism configured to produce a time variant clock value; wherein said programming is further configured to utilize the clock value in producing the encrypted key (col. 10 line 63 to col. 11 line 7).

Referring to claim 35, Pavlov et al. in view of Walker et al. disclose the smart card according to claim 34, Pavlov et al. disclose further a transaction counter configured to produce a transaction count based on a number of transactions performed utilizing the smart card; wherein said programming is further configured to utilize the transaction count in producing the encrypted key (col. 12 lines 29-50).

Allowable Subject Matter

Claim 36 is allowed.

The following is a statement of reasons for the indication of allowable subject matter: "decrypts the encrypted key using a count from a second transaction counter and a second time varying clock value from a second clocking mechanism synchronized with the first clocking mechanism, and authorizes a transaction if the

decrypted key is valid; the decrypted key being valid if produced by the smart card with a valid PIN and the first and second transaction counters are synchronized within a predetermined number of transactions".

Claim Objections

Claims 12, 14-16 and 23 are objected to as being dependent upon a rejected base claim, but

would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Referring to claim 12, the following is a statement of reasons for the indication of allowable subject matter: the prior art fail to suggest limitations that wherein the key confirmation processor approves a transaction if the contents of the first counter matches contents of the second counter within a predetermined range.

Referring to claim 14, the following is a statement of reasons for the indication of allowable subject matter: the prior art fail to suggest limitations that the key confirmation processor is programmed to confirm an authenticity of the key in a manner at least partially dependent upon the contents of the second counter and an output of the second clocking mechanism.

Referring to claim 23, the following is a statement of reasons for the indication of

allowable subject matter: the prior art fail to suggest limitations that maintaining first and second clocking devices configured to respectively produce first and second clock signals; wherein: said step of generating a security key comprises generating a security key in a manner at least partially dependent upon the count and the first clocking device; and said step of confirming the security key comprises confirming that the security key was generated by an authorized user at least in part through use of the second count and the second clock signal.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Shen (US# 6,547,130) disclose an integrated circuit card with fingerprint verification capability.

Any inquiry concerning this communication or earlier communications form the examiner should be directed to Scott Au whose telephone number is (703) 305-4680. The examiner can normally be reached on Mon-Fri, 8:30AM – 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael Horabik can be reached at (703) 305-4704. The fax phone numbers for the organization where this application or proceeding is assigned are (703)-872-3906.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)-305-3900.

Scott Au

MICHAEL HORABIK
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600